

FIGURE 1

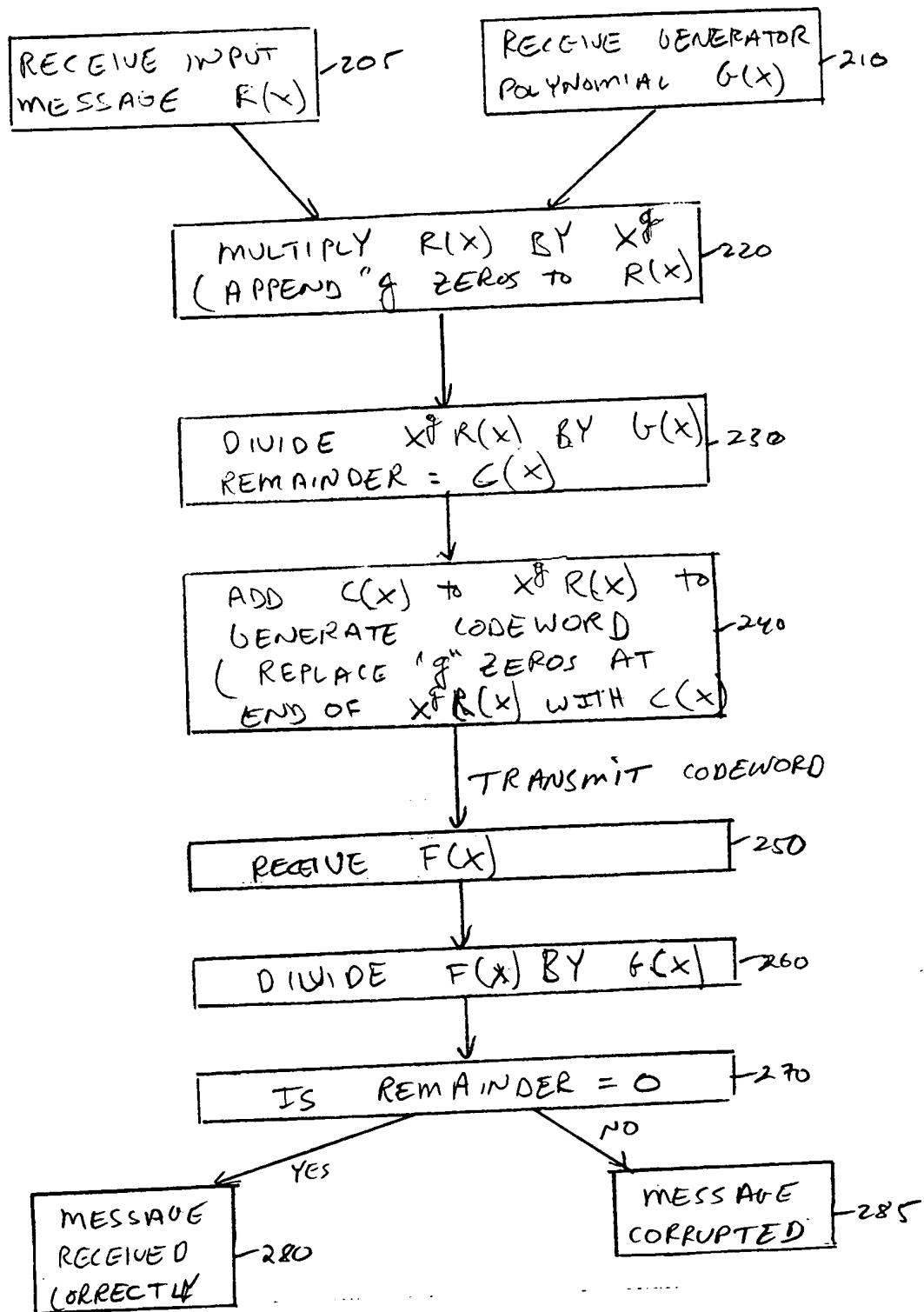


FIGURE 2

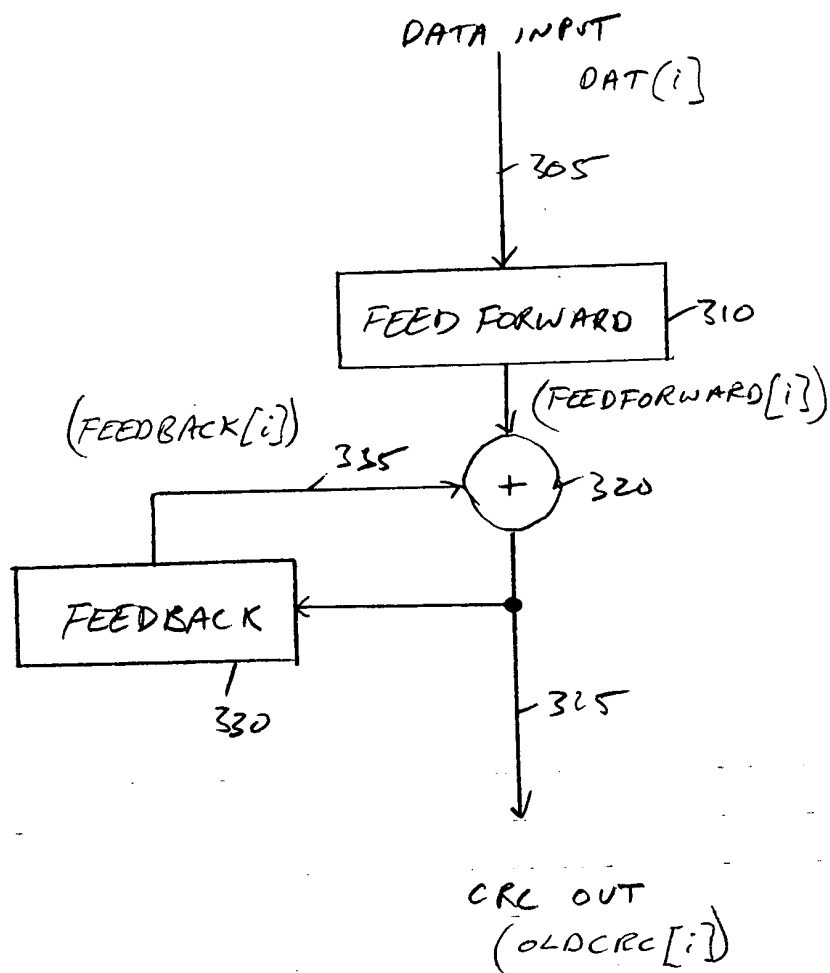


FIGURE 3

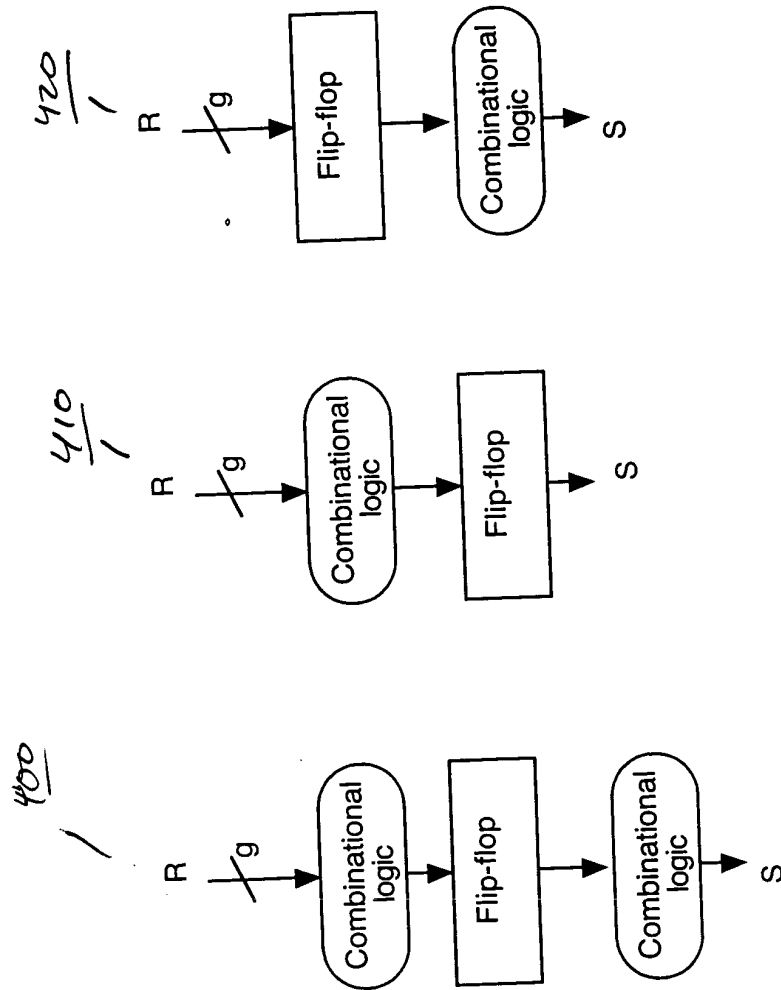


Figure 4

$$x^p(w_1, w_2, w_3) \bmod 6 = x^p(w_1 \cdot x^{2w} + w_2 \cdot x^w + w_3) \bmod 6 \quad \sim 500$$

$$\begin{array}{rcl} (w_1 \cdot x^{2w} + z \cdot x^w + z) \bmod 6 & \sim & 505 \\ (z \cdot x^{2w} + w_2 \cdot x^w + z) \bmod 6 & \sim & 510 \\ (z \cdot x^{2w} + z \cdot x^w + w_3) \bmod 6 & \sim & 515 \\ \hline (w_1 \cdot x^{2w} + w_2 \cdot x^w + w_3) \bmod 6 & \sim & 520 \\ = (w_1, w_2, w_3) \bmod 6 & \sim & 522 \end{array}$$

$$\text{IF: } (w_1) \bmod 6 = s_1 \sim 530$$

$$(w_2) \bmod 6 = s_2 \sim 540$$

$$(w_3) \bmod 6 = s_3 \sim 530$$

$$\begin{array}{rcl} \text{THEN: } (s_1 \cdot x^{2w} + s_2 \cdot x^w + s_3) \bmod 6 & \sim & 560 \\ = (w_1 \cdot x^{2w} + w_2 \cdot x^w + w_3) \bmod 6 & \sim & 565 \end{array}$$

$$\begin{array}{rcl} \text{SO: } (s_1 \cdot x^{2w} + z \cdot x^w + z) \bmod 6 & \sim & 570 \\ (z \cdot x^{2w} + s_2 \cdot x^w + z) \bmod 6 & \sim & 575 \\ (z \cdot x^{2w} + z \cdot x^w + s_3) \bmod 6 & \sim & 580 \\ \hline (w_1 \cdot x^{2w} + w_2 \cdot x^w + w_3) \bmod 6 & \sim & 590 \\ = (w_1, w_2, w_3) \bmod 6 & \sim & 595 \end{array}$$

FIGURE 5

$$x^q \cdot (w_1 w_2 w_3) \bmod b \sim 600$$

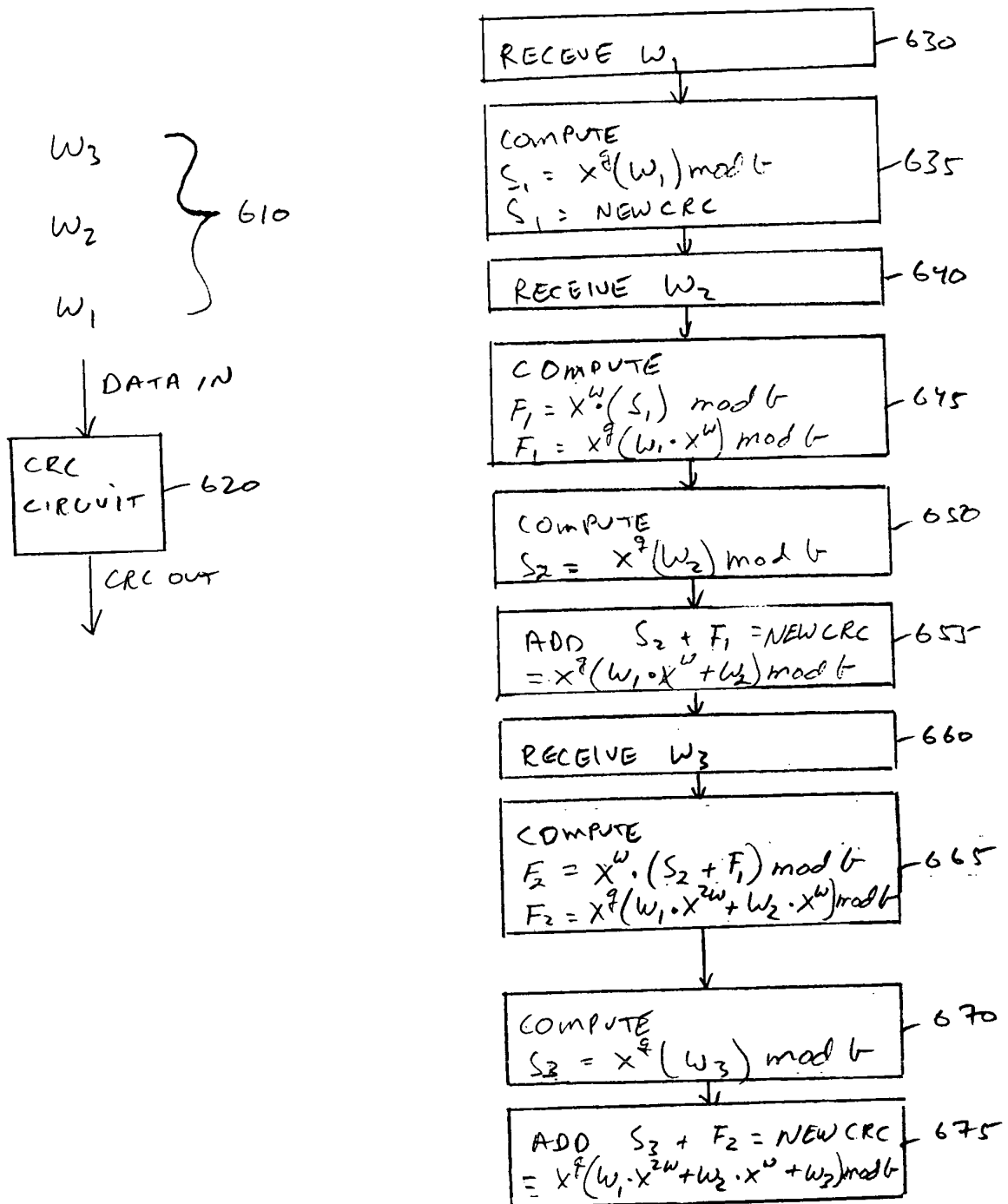


Figure 6

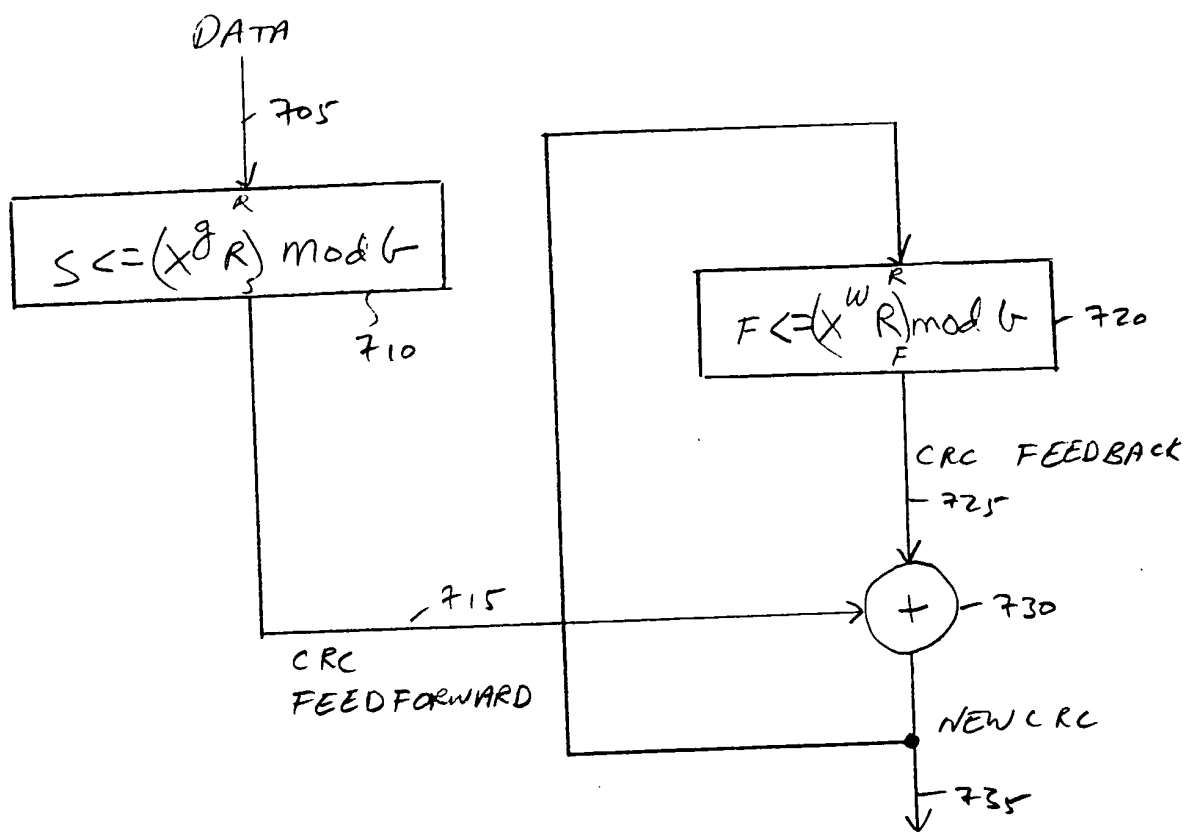


Figure 7

$$x^i(w_4 w_3 w_2 w_1) \bmod b = \underline{800}$$

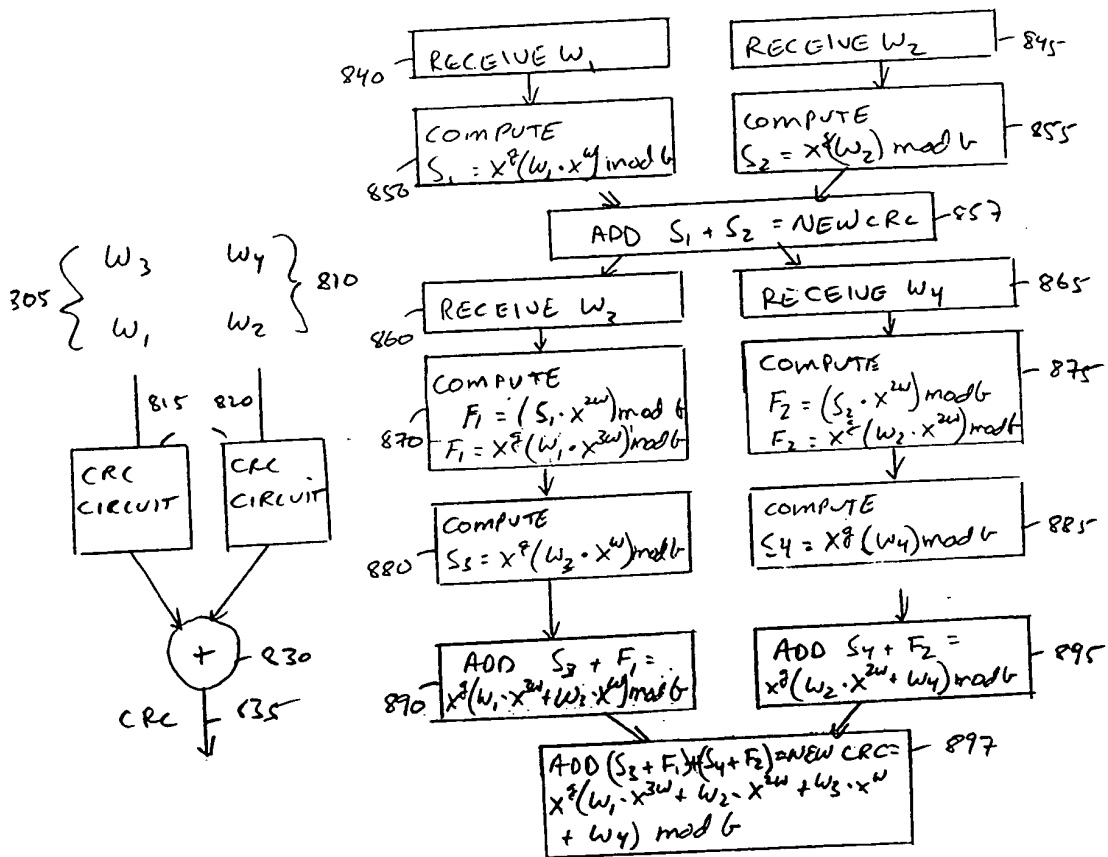


FIGURE 8

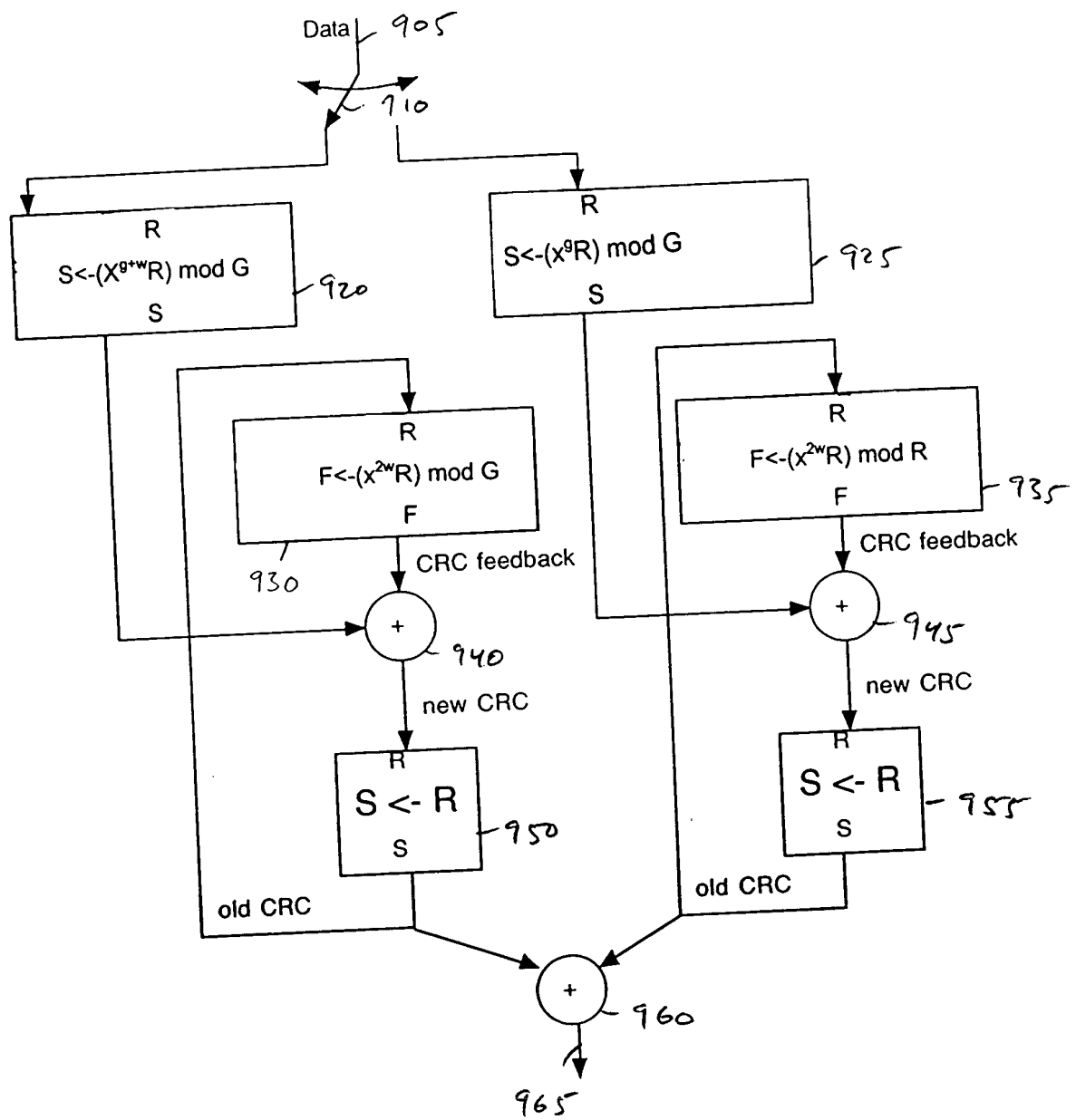


Figure 9

$$x^{\frac{1}{2}}(w_1 w_2 w_3) \bmod 6 = x^{\frac{1}{2}}(w_1 \cdot x^{2w} + w_2 \cdot x^w + w_3) \bmod 6$$

1010

$$\begin{array}{rcl} (w_1 \cdot x^{2w} + z \cdot x^w + w_3) \bmod 6 & \sim & 1015 \\ (z \cdot x^{2w} + w_2 \cdot x^w + z) \bmod 6 & \sim & 120 \\ \hline (w_1 \cdot x^{2w} + w_2 \cdot x^w + w_3) \bmod 6 & \sim & 1075 \end{array}$$

$$\begin{array}{rcl} \text{IF : } (w_1) \bmod 6 = S_1 & \sim & 1030 \\ (w_2) \bmod 6 = S_2 & \sim & 1035 \\ (w_3) \bmod 6 = S_3 & \sim & 1040 \end{array}$$

$$\begin{array}{rcl} \text{THEN: } (S_1 \cdot x^{2w} + z \cdot x^w + S_2) \bmod 6 & \sim & 1045 \\ (z \cdot x^{2w} + S_2 \cdot x^w + z) \bmod 6 & \sim & 1050 \\ \hline (w_1 \cdot x^{2w} + w_2 \cdot x^w + w_3) \bmod 6 & \sim & 1055 \\ = (w_1 w_2 w_3) \bmod 6 & \sim & 1060 \end{array}$$

FIGURE 10

$$x^q (w_1 w_2 w_3) \bmod b = \underline{1100}$$

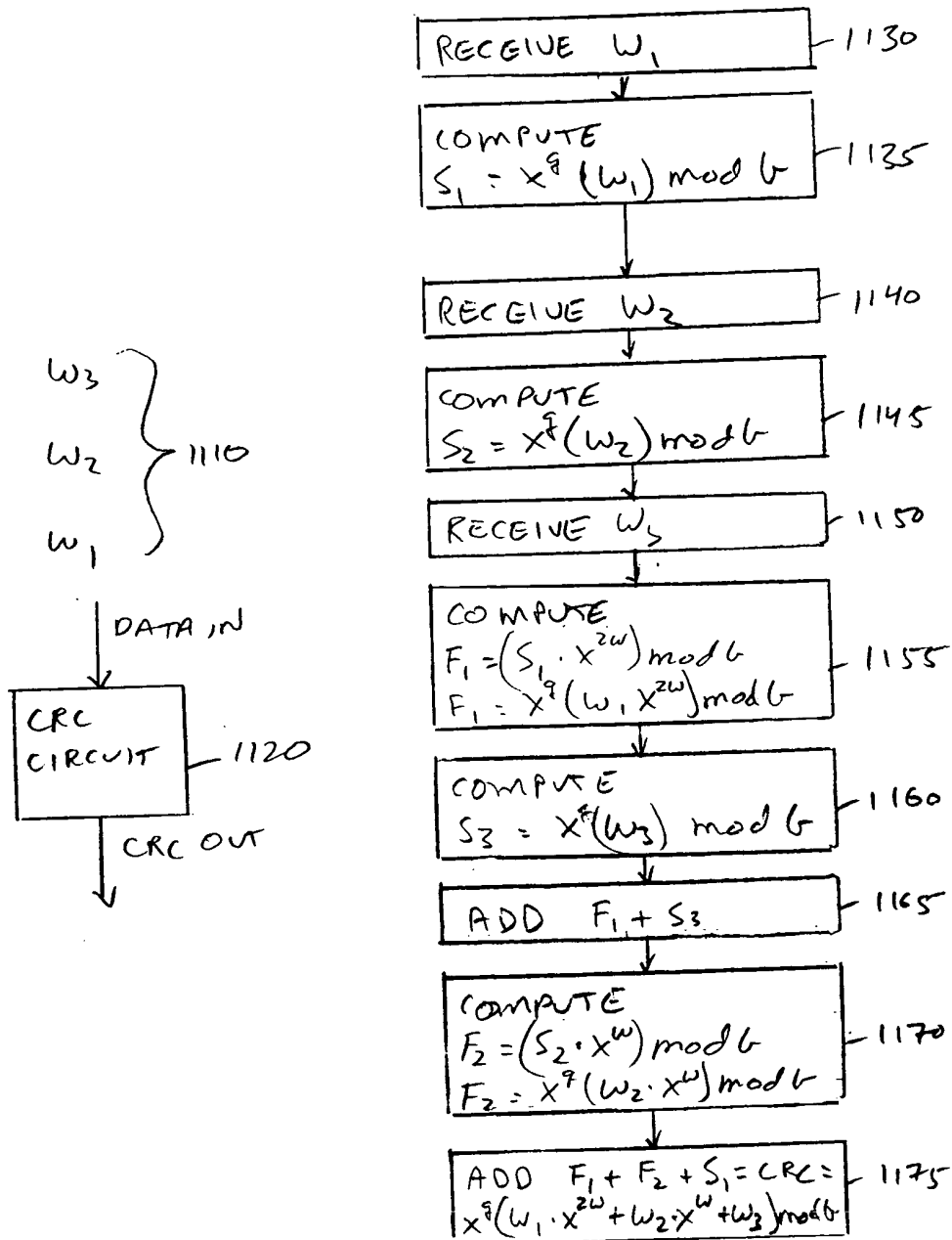
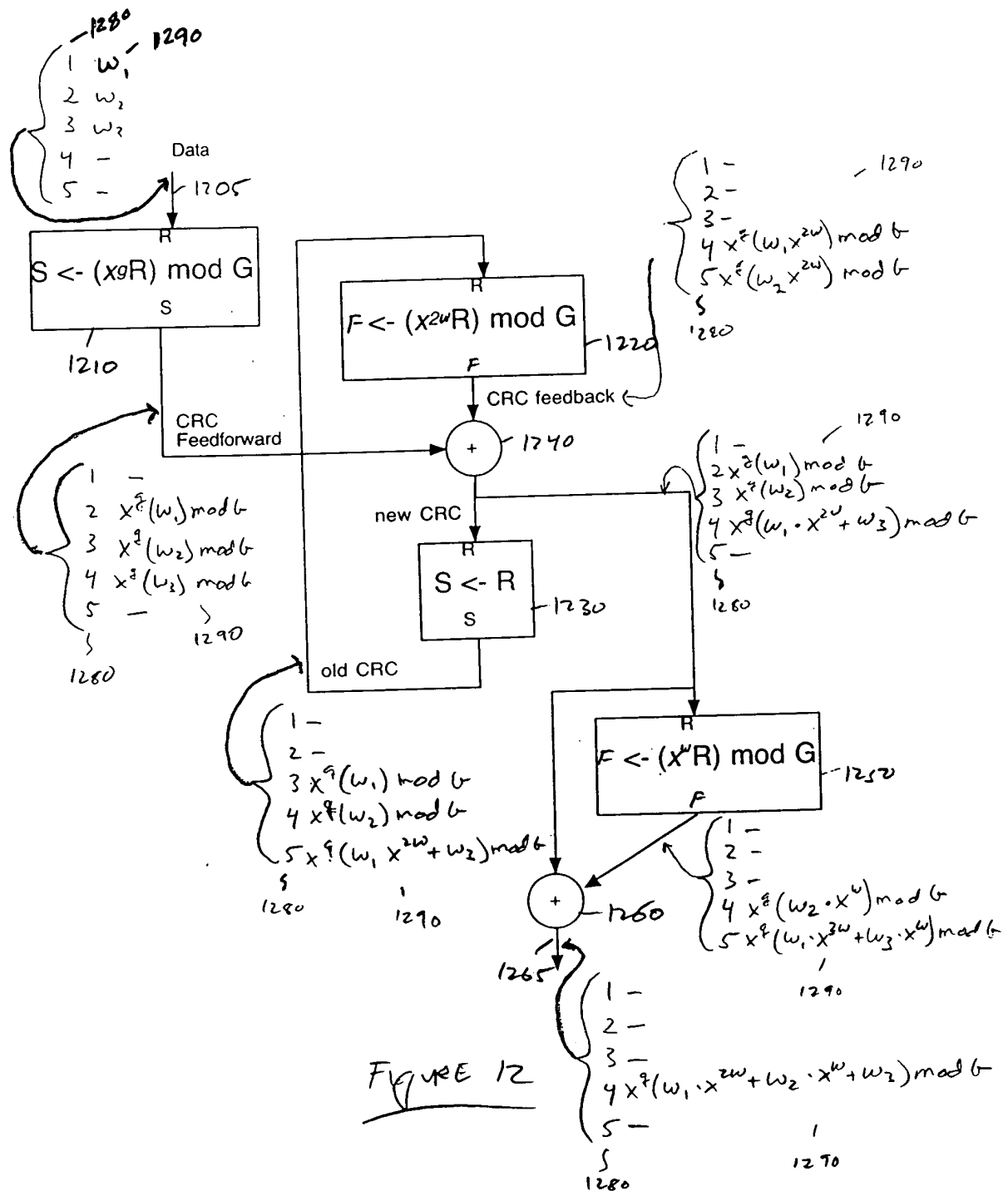


FIGURE 11



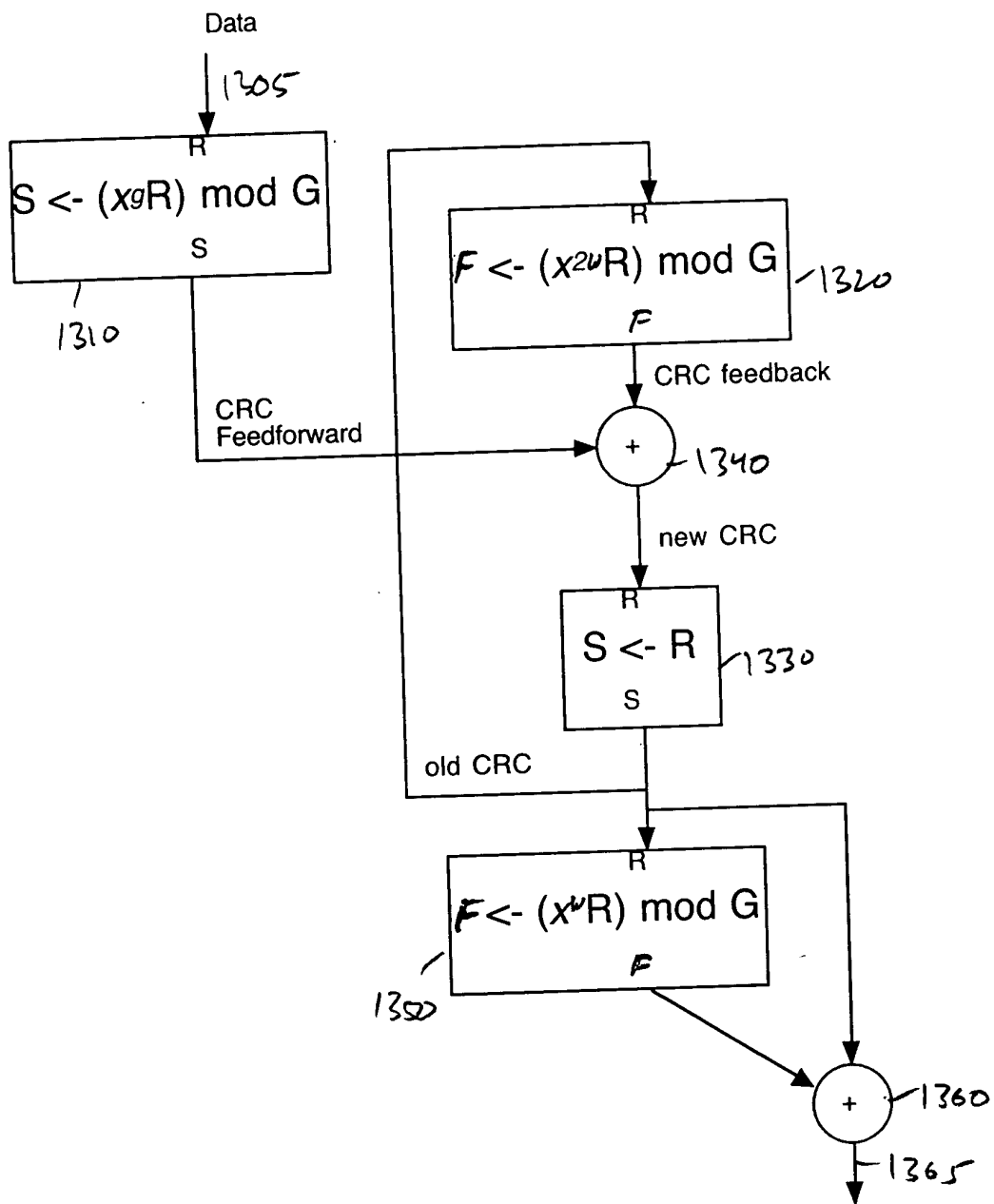


FIGURE 13

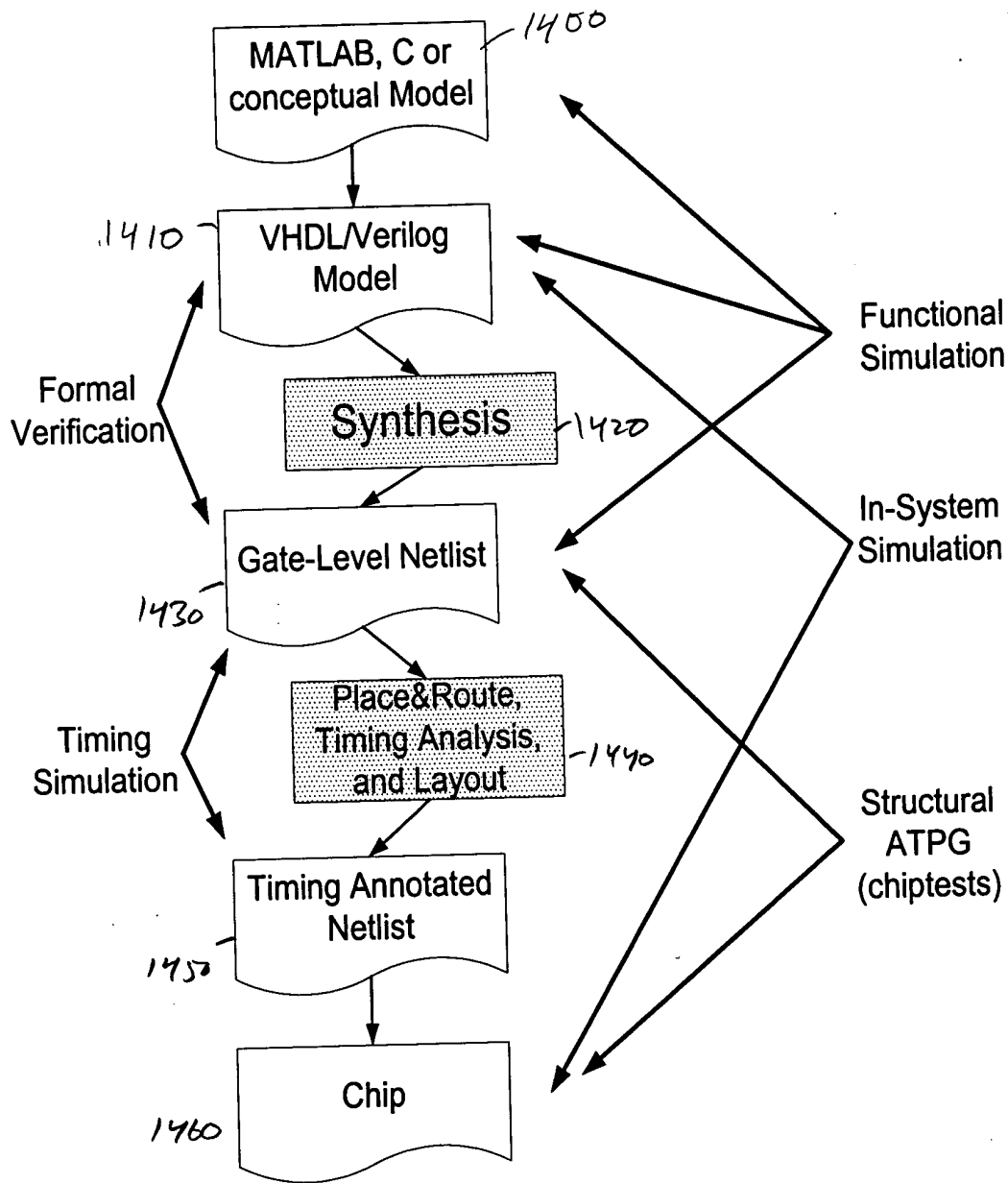


Figure 14

